Independent market research and
competitive analysis of next-generation
business and technology solutions for
service providers and vendors

HEAVY READING

WHITE PAPER

# Security Strategies to Prepare for 5G & IoT

*A Heavy Reading white paper produced for A10 Networks*

AUTHOR: JIM HODGES, PRINCIPAL ANALYST, HEAVY READING

# INTRODUCTION

Communications service providers (CSPs) are undergoing a massive digital transformation. Increasing bandwidth usage per subscriber is powering the demand for new digital content and applications. This transformation is paving the way for the new era of mobile broadband and connected things, including the scalable, hyper-connected Internet of Things (IoT) world. This new world is more susceptible to malicious intrusions, especially with the increasing cybersecurity threat landscape.

For many communications service providers (CSPs), the implementation of strategies such as the deployment of network functions virtualization (NFV) and software-defined networking (SDN) technologies represents an opportunity to significantly shorten the time required to bring new services to market, as well as leverage the dynamic scaling of software resources to most effectively monetize telco services and OTT services running on their network.

This new software strategy must also address the additional security requirements inherent with running applications in a number of locations. Accordingly, in the third quarter of 2017, Heavy Reading, in conjunction with A10 Networks, undertook the creation and execution of a global survey designed to assess cloud, premises, and hybrid network security concerns and evaluate CSPs' strategies to mitigate the risks of a threat curve on an upward trajectory. The key findings from the survey are documented in this white paper.

# THE SECURITY LANDSCAPE

One of the realities of shifting to software in a security context is that it fuels a broad-spectrum attack model. By that we mean, the move to a pure-software distributed application model supporting a myriad of devices provides a much wider landscape for bad actors to exploit for data infiltration or exfiltration.

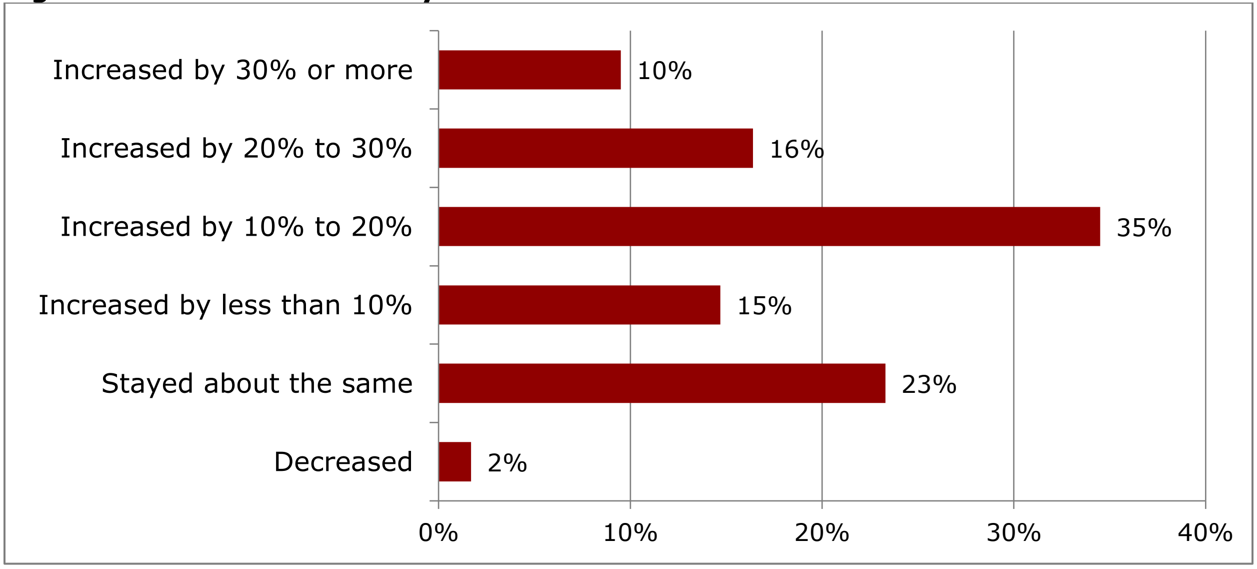
Thus, not only is the landscape a much larger target, but cyberthreats initiating from both inside and outside the network are a much greater concern. Although the threat impact of 5G and IoT devices have yet to even be fully assessed, they certainly will be very significant over the next few years. Moreover, there is little debate that security must be adaptable and programmable to optimally respond to an increasing number of security threats.

And this increase is substantial. As shown in **Figure 1**, the most common response (35% of respondents) was a 10%-20% increase in a 12-month window. After this, 16% of respondents report seeing a 20%-30% increase.

At the upper and lower ends of the scale, 15% reported a 10% increase in incidents, while 10% reported an increase of 30% or more. While 23% said the number of incidents had stayed about the same, just 2% reported that incidents had decreased. A key takeaway here is that 76% of CSPs are experiencing some growth in the number of security incidents, with 61% experiencing significant growth (i.e., 10% or greater).

Moreover, it's not just a numbers game, since threat vectors continue to become more sophisticated and difficult to detect. For instance, the smartphone Mirai bot, which delivered distributed denial of service (DDoS)-driven attacks in 2016, has morphed into Persirai, which targets IP cameras. This evolution is important because it highlights that the push to "weaponize" 5G and IoT devices will be relentless and ongoing, just as it has been with 4G.

**Figure 1: Number of Security Incidents**



*Question: How has the number of cybersecurity incidents changed at your company over the past 12 months? (N=117)*
*Source: Heavy Reading/A10 Networks Custom Survey 3Q17*

Essentially the security concerns associated with 5G and IoT are twofold. The first concern is increased device intelligence. For example, in a 5G context, 5G defines user equipment (UE) to reflect the fact that a single device may be programmed to support several distinct network slices, including non-traditional applications.

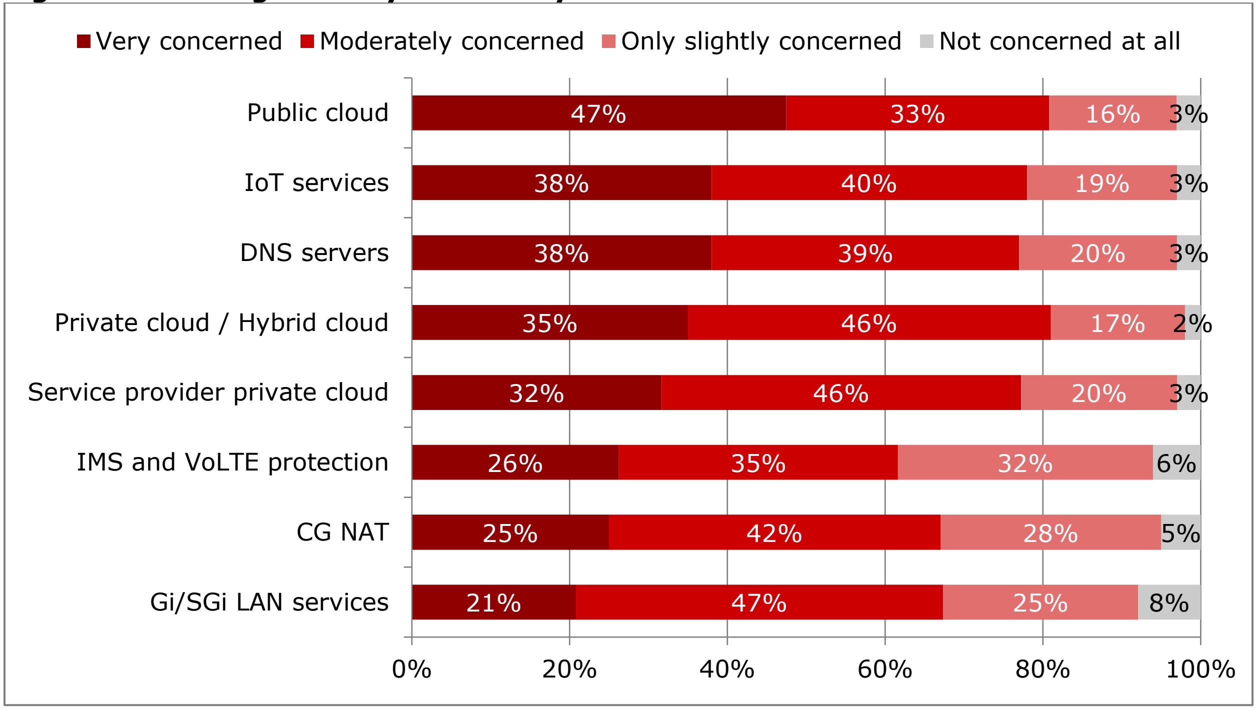
Another consideration here is the billions of IoT devices, which must be individually managed as unique network slices. Accordingly, to manage these devices, it is now clear that there must be a greater focus on implementing automated security policies that can make decisions on machine speeds and possess not only a centralized view of which applications are running, but also much deeper insight into the individual application profiles.

This centralized view is critical, since applications such as IoT will not only run in a distributed cloud framework, they may ultimately even execute in a multi-cloud or on-premises framework, which amplifies the intrusion risk. This reality was reflected in the input from the survey respondents.

For instance, as shown in **Figure 2**, CSPs are "very concerned" about security on several fronts. Of these, the greatest concern is applications running in the public cloud (47%), followed by the risk of IoT applications and securing Domain Name System (DNS) servers (both 38%), and then securing private and hybrid clouds (35%) and their dedicated service provider cloud (32%).

Given such a broad range of concerns, new approaches and strategies for managing pure software-based applications are mandatory. While the requirements are still quite dynamic, there is widespread agreement that any strategy will rely heavily on automation and analytics to enforce security policies and to support a level of enhanced application visibility that doesn't exist today. Stated differently, whichever software configuration (e.g., cloud, on-premises or hybrid) is supported, it's crucial that visibility is not segregated, but that there is a centralized, aggregate view of what is happening on an application level.

**Figure 2: Ranking Security Threats by Network Level**



*Question: How concerned is your company about potential security threats to the following network infrastructure and services? (N=116-117)*
*Source: Heavy Reading/A10 Networks Custom Survey 3Q17*

Still, it's important to also be pragmatic in the implementation of these strategies. By that we mean, CSPs have made very significant investments in network elements such as application delivery controllers (ADCs), web application firewalls (WAFs) and carrier-grade NAT (CGNAT), which must be protected. However, these products must also evolve to the new realities of the software era. In the first instance, they must support enhanced scale metrics, given that attacks are now often volumetric in nature, requiring a solution that can manage millions of simultaneous flows.

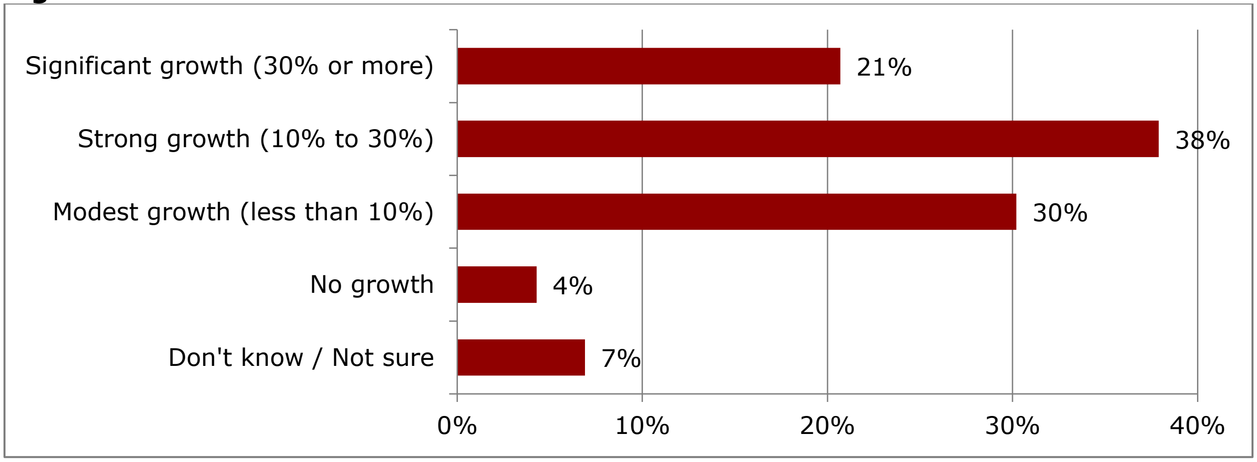
Secondly, these solutions must support a greater level of integration with other network functions, as well as automation and analytics platforms to provide the vital level of application visibility needed to enforce security policies to respond to attacks on the network infrastructure. Furthermore, a consolidated security approach is essential to mitigate attacks such as WireX botnet DDoS application-layer attacks from infected devices, Internet-initiated attacks targeting the Evolved Packet Core (EPC), IMS and DNS servers, or (D)DoS attacks from roaming partners on the GPRS Tunneling Protocol (GTP).

## THE IMPACT OF IoT

As we have documented, IoT is a security game-changer on several levels. While CSPs will benefit from supporting IoT applications and network slices on their networks, the security implications are significant and will have a major impact on security enforcement and policies. This is in large part because IoT attacks can now be launched by infected devices both externally and internally.

Accordingly, as the number of IoT devices grows, so will the threat level. While it is still early in the commercial ramp, as shown in **Figure 3** the growth of IoT devices is now already a factor, with nearly 60% of the survey respondents anticipating "strong" (10% to 30%) growth or "significant" (30% or more) growth within a 12-month window. Specifically, 38% anticipate strong growth, while 21% anticipate significant growth. Given the billions of devices IoT represents, these numbers are sobering and reflect the fact that IoT security strategies must be implemented immediately, before the device numbers become unmanageable from a security perspective.

**Figure 3: IoT Device Growth in Next 12 Months**



*Question: What level of growth in the number of IoT devices on your network do you expect over the next 12 months? (N=116)*
*Source: Heavy Reading/A10 Networks Custom Survey 3Q17*

However, as previously touched upon, it's not just the number of devices from an intrusion perspective, but also the performance requirements that must be considered. Since these devices have unique performance requirements and profile compositions, diverse policies will be necessary to manage IoT devices from a security visibility perspective. This means that a new level of visibility will be necessary to tailor performance and access to security requirements, given that IoT devices will most certainly be targeted by bad actors to launch several attack types (e.g., DDoS). Specifically, what is needed is a programmable, application-aware security strategy that is scalable to manage high numbers of concurrent connections and connections per second with full-spectrum attack protection.

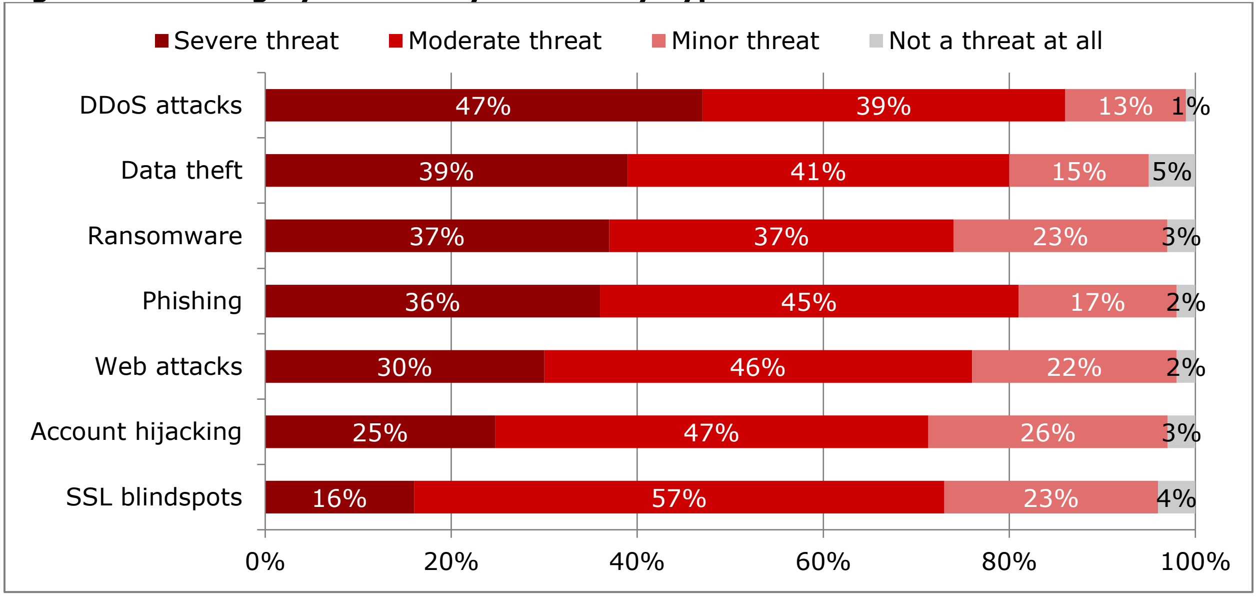
Moreover, IoT attacks can have a wider breadth of attack capabilities than traditional threats. For example, traditional attacks targeting DNS servers are conceptually straightforward to defend against, since the DNS represents a single attack point. In contrast, IoT attacks are much broader and capable of leveraging millions of devices, such as game controllers or even home security controllers, to create DDoS attacks of enormous scale in minutes. The other side of the scale discussion is the requirement to be able to quickly provision and authenticate IoT devices to ensure market competitiveness for new IoT services, as well as the ability to carry a large number of concurrent connections with full-spectrum attack protection.

The complexity of this attack protection model should not be understated and represents another reason why the implementation of an application-aware security visibility model is necessary. For example, IoT attacks don't rely on spoofing to create wide attacks; instead, they are real endpoints with real IP addresses, making it more difficult to block each individual device that is sending attack traffic. Additionally, IoT attacks are widely distributed globally, and each IP must be treated differently, because one cannot simply block the IP range of a network segment or entire country to block a small subset of threat vectors.

## THE EVOLUTION OF THE THREAT LANDSCAPE

Given the considerations discussed in the previous sections, it's fair to conclude that the threat landscape has already made at least one evolutionary turn to a broader and more complex threat landscape, with future evolutions sure to follow. To perform a level-set, we asked the survey respondents to rank the greatest threats they currently face. Of these, as shown in **Figure 4**, based on "severe threat" responses, the top four concerns are DDoS attacks (47%), followed by data theft (39%), ransomware (37%) and phishing attacks (36%).

**Figure 4: Ranking Cybersecurity Threats by Type**



*Question: Please rate the following types of cybersecurity threats to your company. (N=116-117)*
*Source: Heavy Reading/A10 Networks Custom Survey 3Q17*

The threat rankings provided by the respondents are interesting on several levels. First, the input clearly shows that DDoS attacks represent the greatest threat type, aligned with the IoT discussion above. However, the relatively close grouping of the scores of other threats confirms that many threats are in play – ones that represent both internal and external multi-vector attack types. Therefore, the key finding here can only be that the threat landscape is diverse, potent and subject to both internal and external stimuli.

While CSPs will need to upgrade their security network capabilities to provide protection against DDoS attacks (including IoT-driven DDoS attacks), given the multi-cloud hybrid cloud model noted (see **Figure 2**), best practices will also require a hybrid implementation approach that supports an on-premises mitigation solution, combined with a cloud-based solution for the broadest level of DDoS detection.

By this, we mean that to completely insulate some applications from DDoS attacks, in many cases a mix of cloud and on-premises security solutions will be required to manage service and application execution. In turn, this will mean the pushing of policy enforcement and application visibility beyond the cloud itself, which represents a sea change in how CSPs currently manage security enforcement. To accomplish this shift, CSPs must focus on application visibility and move away from the traditional method of identifying applications by port number and protocol and move to an automated analytics model that can invoke policy enforcement based on malicious applications, malicious URLs and even infected content.

## THE RISE OF ANALYTICS

There is little debate that analytics now represents a vital capability for securing the threat landscape. Encrypted traffic presents a significant security challenge to organizations, as the complexities of monitoring and uncovering threats can be daunting. Maintaining a decrypt zone to eliminate the network blind spot and inspect the encrypted traffic, as well as to provide granular analytics for the application in a multi-cloud environment, is key to a robust security strategy. While analytics can provide invaluable insight on an individual level to enable policy execution, the advance and rise of analytics, in conjunction with artificial intelligence (AI), is important because it provides CSPs with predictive analytics capabilities that push beyond basic threat *management* to threat *prevention*.

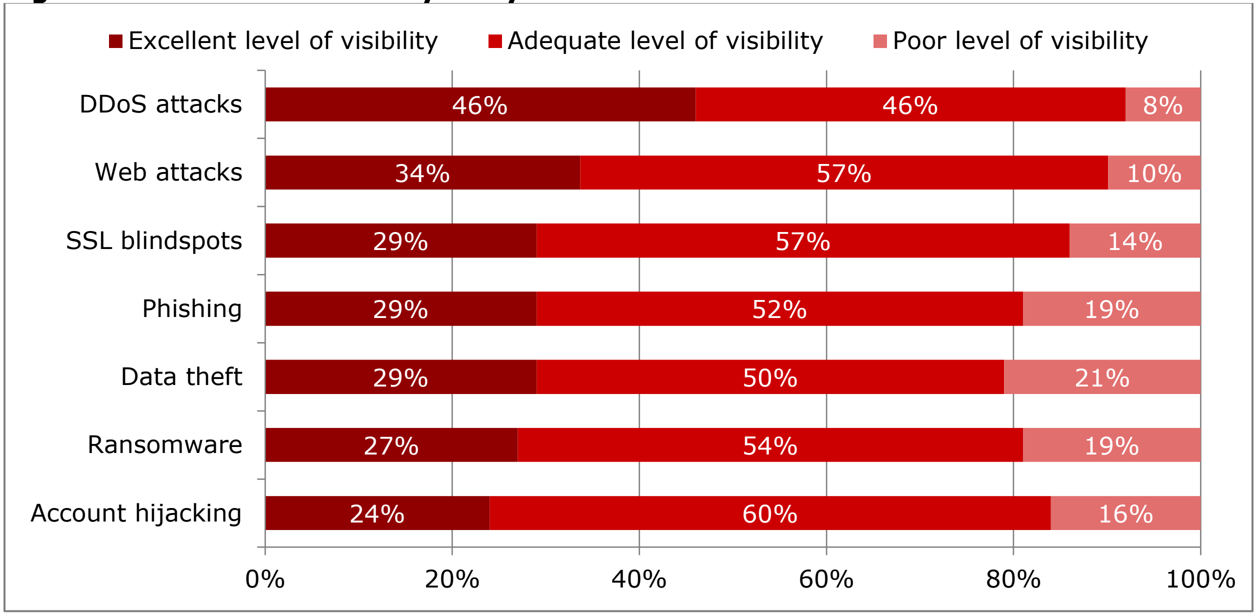
This is an important step, since many threats, like bots themselves, are moving to an automated model to enable them to better adapt to changes in security perimeter enforcement. Fortunately, over the last few years, the industry has seen major advances in analytics. While vendors' products historically provided basic metrics, the data available today is more granular and more actionable. An example is A10 Networks, which supports centralized management across traditional on-premises data centers, public, private and hybrid clouds, with advanced analytics capabilities aligned with this automation-driven prevention model (see **About A10 Networks**, below).

At the same time, application development teams are now designing applications to provide a much greater level of insight into application performance. This is also an important step, because it facilitates the move to the per-application security enforcement model. Therefore, in this new model, predictive analytics systems will have insight into the behavior of the infrastructure, applications and clients to recognize anomalous performance or security behavior, and when an application or server is going to fail. Once that behavior is noticed, automated policies can remediate the potential problem (e.g., transferring traffic to another server or load-balancing the application).

Encouragingly, as shown in **Figure 5**, this new approach is starting to pay dividends. For example, nearly half (46%) of CSPs feel that they now have an "excellent level of visibility" into the greatest threat type – DDoS attacks. Still, the relatively low level of excellent visibility metrics for other cyberattack types – e.g., data theft (29%) and ransomware (27%) – confirm that CSPs need to step up the execution and broaden the deployment of analytics-driven visibility into their networks to support the real-time prevention model.

The transition to an analytics-enabled automated security model also has ramifications on the type of security measures implemented and where they will be enforced. This discussion includes the shift to the application-aware rather than the port number enforcement model. Specifically, this refers to utilizing analytics to empower security enforcement on a per-application basis.

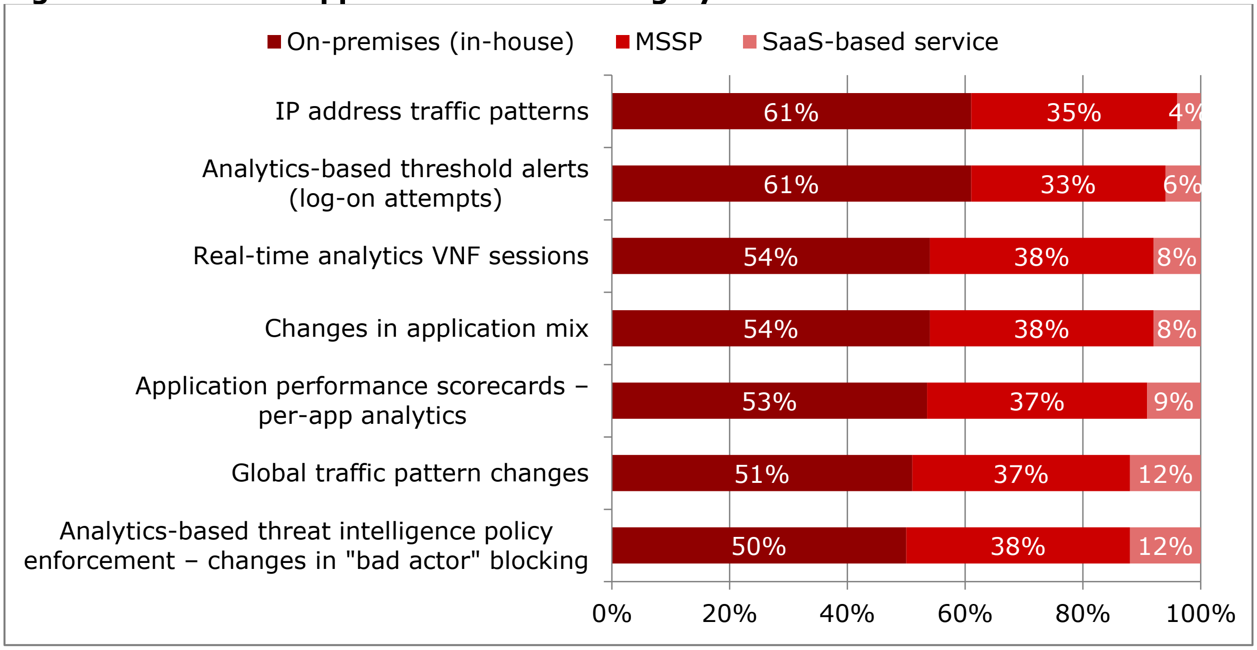
**Figure 5: Real-Time Visibility of Cyberattacks or Threats**



*Question: What level of real-time visibility does your company have into the following types of cyberattacks or threats? (N=115-117)*
*Source: Heavy Reading/A10 Networks Custom Survey 3Q17*

Consequently, as shown in **Figure 6**, looking at a broad list of the holistic capabilities that analytics supports in a security context, it's clear that most CSPs wish to maintain in-house control so they can optimize security outcomes by enhancing their level of threat visibility.

**Figure 6: Preferred Approaches for Handling Cyberattacks**



*Question: What is your company's preferred approach for implementing the following analytics capabilities to secure applications? (N=115-116)*
*Source: Heavy Reading/A10 Networks Custom Survey 3Q17*

While about a third of respondents (33%-38%) are willing to rely on third-party managed security service providers (MSSPs), more than half (50%-61%) prefer to maintain in-house control of analytics capabilities.

We believe there are several factors at play driving the internal control model. Of these, a leading consideration is the business opportunity related to IoT, 5G network slicing, which presents value-added upsell tailored opportunities on a per-application basis. Since CSPs are not likely to cede control of applications, they also perceive maintaining responsibility for security enforcement leveraging an application insight model as core and fundamental to the execution of cloud business strategies.

## CONCLUSION

CSPs now find themselves facing a very different threat landscape from only a few years ago. The truth of today's software-empowered world is that for security to be effective, it must deliver unprecedented levels of network visibility – visibility that encompasses network performance, but also visibility into the very applications that traverse IoT network interfaces or 5G network slices.

In response, as we have documented, CSPs are now taking critical steps and revising security strategies through the adoption of analytics and integrated automated security policies designed to meet their immediate security requirements and those that lie within plain sight on the threat horizon.

## ABOUT A10 NETWORKS

A10 Networks enables intelligent automation with machine learning to ensure that business-critical applications are protected, reliable and always available.

A10 is a leader in application networking and security, providing a wide range of high-performance carrier-grade solutions that help service providers scale and secure their network infrastructure to meet the demanding requirements of current and next-generation 3G/4G LTE/5G networks and IoT deployments. A10's security and cloud portfolio addresses DDoS protection, orchestration, management and analytics. A10's products come with built-in security features including integrated DDoS protection to self-protect the device, and service resources to help assure service continuity and brand credibility.

Additionally, A10's cloud solution is built on microservices and container technologies, providing centralized agile management, automation and analytics for secure services in any application environment – deployed across data centers, private and public clouds. A10's RESTful API integrates with the various CI/CD tools such as Ansible, Jenkins, SaltStack, Chef and Puppet, enabling service providers to streamline capacity planning, while reducing the total cost of ownership (TCO).